United States District Court

NORTHERN DISTRICT OF TEXAS

UNITED STATES OF AMERICA

v.

JESSE WILLIAM MCGRAW
also known as GhostExodus, PhantomExodizzmo,
Howard Daniel Bertin, Howard William McGraw,
and Howard Rogers
2801 Trinity Oaks Dr, Apt 328
Arlington, Texas, 76001

CRIMINAL COMPLAINT

CASE NUMBER: 3:09-MJ-207

I, the undersigned complainant being duly sworn state the following is true and correct to the best of my knowledge and belief. Between April 2009 and June 2009, in Dallas, Dallas County, in the Northern District of Texas **JESSE WILLIAM MCGRAW** did,

knowingly cause the transmission of a program, information, code, or command, in that **MCGRAW** downloaded a malicious code into a computer located at 9301 North Central Expressway, Dallas, Texas, the building that houses the Carrel Clinic, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer, and the harm threatened public health and safety.

in violation of 18 U.S.C. §1030(a)(5)(A) and §1030(c)(4)(B)(iv).

I further state that I am a Special Agent of the Federal Bureau of Investigation and that this complaint is based on the facts set out in the attached affidavit.

Continued on the attached sheet and made a part hereof. (X) Yes ( ) No

Ajeet Singh, Special Agent
Federal Bureau of Investigation

Based upon this complaint, this Court finds that there is probable cause to believe that an offense has been committed and that the defendant has committed it. Sworn to before me, and subscribed in my presence

JUNE 26, 2009 at Dallas, Texas
Date City and State

JEFF KAPLAN
United States Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF COMPLAINT

I, Ajeet Singh, having been duly sworn, depose and state as follows:

1. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been so employed for approximately 5 years. I am currently assigned to the Dallas Office of the FBI, and my duties include the investigation of computer intrusions, theft of trade secrets violations, copyright and trademark infringement violations, and high-tech fraud. I have received specialized training in the field of computer intrusions and intellectual property crimes.

2. I make this affidavit in support of an application by the United States of America for the issuance of a complaint and arrest warrant for

JESSE WILLIAM MCGRAW, residing at 2801 TRINITY OAKS DR, APT 328 ARLINGTON, TEXAS, 76001, Texas Driver's license number 22501049, Social Security Number 549-93-3224, also known as Howard Daniel Bertin, Howard William McGraw, Howard Rogers, and various combinations of those first, middle, and last names.

3. As set forth herein, there is probable cause to believe that **JESSE WILLIAM MCGRAW**, also known as **PhantomExodizzmo** and **GhostExodus**, leader of the group "Electronic Tribulation Army" along with others individuals known and unknown to the government have conspired to engage in and/or did engage in a computer intrusion, in violation of 18 U.S.C. § 1030.

APPLICABLE CRIMINAL STATUTES AND DEFINITIONS

4. There is probable cause to believe that **JESSE WILLIAM MCGRAW** has violated the provisions of 18 U.S.C. §1030(a)(5)(A) and §1030(c)(4)(B)(iv).

> **1030(a)(5)(A)** Whoever . . . knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer..
>
> **1030(c)(4)(B)(i)** the punishment for an offense under subsection (a) . . . of this section is - a fine under this title, imprisonment for not more than 10 years, or both, in the case of - an offense under subsection (a)(5)(A) which does not occur after a conviction for another offense under this section, if the offense cause . . . a harm provided in subclauses (I) through (VI) of subparagraph (A)(iv), [that being **(iv)**], a threat to public health or safety;

a. Per 18 U.S.C. §1030(e)(2), a "protected computer" is a "computer . . . which is used in or affecting interstate or foreign commerce or communication."

b. "Damage" is defined as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. §1030(e)(8). Although this definition is broad and inclusive, as the use of the word "any" suggests, the definition differs in some ways from the idea of damage to physical property. This definition contains several concepts that allow §1030(a)(5) to apply to a wide variety of situations.

c. First, "damage" occurs when an act impairs the "integrity" of data, a program, a system, or information. This part of the definition would apply, for example, where an act causes data or information to be deleted or changed, such as where an intruder accesses a computer system and deletes log files or changes entries in a bank database.

d. Similarly, "damage" occurs when an intruder changes the way a computer is instructed to operate. For example, installing keylogger software on a home computer can constitute damage. Damage also occurs if an intruder alters the security software of a victim computer so that it fails to detect computer trespassers. Directing a computer to alter or modify

e. In addition to the impairment of the integrity of information or computer systems, the definition of damage also includes acts that simply make information or computers "unavailable." Intruders have devised ways to consume all of a computer's computational resources, effectively making it impossible for authorized users to make use of the computer even though none of the data or software has been modified.

AFFIANT'S INFORMATION

5. I make this affidavit in part on:

a. personal knowledge based on my participation in an investigation into the activities of **JESSE WILLIAM MCGRAW**,

b. upon oral and written reports provided to me by a confidential witness who I believe to be truthful and reliable as set forth herein, and to have a sufficient basis of knowledge/access to the information that was provided to me,

c. upon the information provided to me by other law enforcement personnel,

d. upon the information provided to me by Michelle Morris, the property manager for 9301 North Central Expressway, Dallas, Texas,

e. upon information provided by a Cooperating Witness (CW-1),

f. upon information provided to me by the property manager of the Trinity Oak Apartments, and,

g. upon my knowledge and experience.

Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1030 are presently located at **2801 TRINITY OAKS DR, APT 328 ARLINGTON, TEXAS, 76001**. Facts not set forth in the affidavit are not being relied upon for probable cause.

FACTS IN SUPPORT OF AFFIDAVIT

6. On 6/24/2009, The Dallas Division of the FBI was contacted by Special Agent Charles Provine of the FBI in the Jackson Division of the FBI regarding a computer intrusion of a Heating Ventilation and Air Condition (HVAC) computer system at a Dallas, TX hospital, the Carrell Clinic located at 9301 North Central Expressway, Dallas, Texas. This was believed to present a risk to health and safety as the Hospital was a facility that kept patients around the clock who could be adversely affected by the cooling if it were turned off during Texas summer weather conditions and the hospital also maintained drugs which could be adversely affected by the lack of proper cooling if the intruder were to disturb the HVAC system. SA Provine stated that he was in contact with Lieutenant (LT) Lannie Hilbolt, Texas Attorney General's office and CW-1, a network

security researcher, who had reported the crime. SA Provine provided affiant with contact information for LT Hilbolt and CW-1. Both SA Provine and LT Hilbolt believe CW-1 to be reliable as they were able to verify the information that CW-1 provided to them. In addition, SAs Allyn Lynd and Ajeet Singh have independently corroborated information reported by CW-1.

Lieutenant Lannie Hilbolt's Summary:

7. On 6/24/2009, affiant contacted LT Hilbolt who provided additional details on the computer intrusion. LT Hilbolt, stated that his office had identified the individual **JESSE WILLIAM MCGRAW, 2801 TRINITY OAKS DR, APT 328, ARLINGTON, TEXAS, 76001**, as having compromised the HVAC system at the CarrellClinic, a medical facility providing health services at 9301 Central Expressway, Dallas, TX, located in the Northern District of Texas. LT Hilbolt stated that he had information that **JESSE WILLIAM MCGRAW,** who used the online nickname **GhostExodus**, had posted pictures on the Internet of the compromised HVAC system and videos of himself compromising a computer system in a hospital. LT Hilbolt stated that he had reviewed records that indicated that **MCGRAW** was planning on using his compromised systems to commit additional crimes on or before July 4, 2009, a date that **MCGRAW** had called Devil's Day.

8. LT Hilbolt provided a summary of his investigation, including a report from CW-1. This summary stated that CW-1 had been contacted via MSN Messenger, an online

instant messaging service, by an individual using the "handle" or alias of XxxxImmortalxxxX. XxxxImmortalxxxX bragged to CW-1 "about getting into a hacker group" called Electronik Tribulation Army (ETA) by showing [the existing members of ETA] pictures of XxxxImmortalxxxX getting into an HVAC system. XxxxImmortalxxxX sent CW-1 links to the screenshots of the HVAC system. From the screenshots CW-1 was able to identify the system as belonging to the Carrell Clinic in Dallas, TX, and verified this from a photo on the Carrell web site. At this point, CW-1 conducted Google searches on ETA. Those searches indicated that a hacker with the handle "**GhostExodus**" was the leader of ETA . Further searches using Google for **GhostExodus** provided CW-1 with links to the "warezscene" and "anarchistcookbook" forums where **GhostExodus** had made posts bragging about hacking the same HVAC system. A forum is a type of web bulletin board where members can exchange communications which can be read by anyone visiting the bulletin board. Both of these forums are known by law enforcement to be frequented by individuals who commit fraud relating to computers. The posts by **GhostExodus** included screenshots which displayed the same Uniform Resource Locator (URL) (also known as web sites) as XxxxImmmortalxxxX provided to CW-1. The URLs were to a photobucket account with several other images which CW-1 found by Googling (using the search engine Google) a partial URL that belonged to **GhostExodus**. Photobucket is an online photo album service. The matching URLS confirmed to CW-1 that XxxxImmortalxxxX was using images that he had seen while joining ETA to impress CW-1. CW-1 believed based on these images that **GhostExodus** was the actual hacker behind the Carrell HVAC

compromise. CW-1 then attempted to identify **GhostExodus** from publicly available information on the Internet. CW-1 claims that CW-1 has a history of successfully performing incident response, a phrase in the computer security industry which means a response to a suspected computer intrusion to determine who conducted the intrusion, what occurred during the intrusion, and how best to repair the damage caused by the intrusion. LT Hilbolt was able to verify this with some of the victims that CW-1 has claimed to assist in the past. CW-1 conducted additional searches on the Internet for "**GhostExodus**" and variations (e.g. "Ghost Exodus" with a space) and "Electronik Tribulation Army". CW-1 located a "Texas Fire Sale" post with a screenshot (a snapshot or capture of the way a computer screen appears to the viewer at a particular point in time) of what appeared to CW-1 to be a compromised municipal system, **GhostExodus**' youtube/blip.tv accounts, other images on **GhostExodus**' photobucket account, **GhostExodus**' vampirefreaks.com account including his photo gallery, Craigslist ads, Myspace accounts, and ETA forums. CW-1 identified an IP address in a video located at **GhostExodus**' http://**GhostExodus**.blip.tv/ account. This video appeared to be a recording of a computer screen while **GhostExodus** demonstrates software used to commit computer intrusion that **GhostExodus** was distributing. In the background of the video, CW-1 observed that **GhostExodus** was using mIRC (an Internet Relay Chat client) to connect to an IRC server. In the process of connecting, the video displays a partial computer name for the local computer on the screen. By downloading the video and slowing it down, CW-1 claimed that CW-1 was able to pause it when the hostname was on the screen and that the hostname started with "ppp-70-251-

119-168". This corresponds with a naming scheme where the first part of the hostname has the IP address in it. CW-1 confirmed this by doing a reverse-DNS lookup on the IP address 70.251.119.168. This returned the complete hostname "ppp-70-251-119-168.dsl.rcsntx.swbell.net". CW-1 also located a screenshot with a much clearer IP/Hostname (70.251.72.165). From the videos on **GhostExodus**' Youtube (an online video storage service) account and his Craigslist post (Craigslist is an online classified ad service), it appeared to CW-1 that **GhostExodus** was probably a night-shift security guard stationed at the Carrell Clinic. CW-1 located Youtube videos showing **GhostExodus** infecting computers at what **GhostExodus** claims in the video to be a business that **GhostExodus** "infiltrated." CW-1 noted that items in the background of this video appear to be from a health clinic, including diagrams, charts of the human body, etc.. CW-1 stated that in the "infiltration" video, **GhostExodus** appeared to be wearing a grey hoodie over his security guard uniform. In another video **GhostExodus** claims that he is at work. In this video, **GhostExodus** showed off what **GhostExodus** described as his "hacker gear", including a cell phone jammer, lockpicks, and fake FBI credentials. CW-1 also told LT Hilbolt that CW-1 believed that **GhostExodus** was trying to take down some of the information about himself on or about 6/23/2009. CW-1 noted that **GhostExodus** had abandoned other sites linked from Google in the past and that this destruction of records could be an attempt to prevent another hacker from "digging up dirt on **GhostExodus**. CW-1 told LT Hilbolt that **GhostExodus** made the following changes to information previously stored online: "He has replaced many of his incriminating posts on the "Anarchist Cookbook" site to

read "Information N/A Thanks". His myspace.com account "blackfridaynull" has been set to "private", meaning that only friends can view it. The http://www.defconsystem.tk/ domain name no longer points at the ETA website. [That] domain used to redirect to http://etapub.webs.com/ , which [was] still active at the moment. The ETA forums at http://hackthebox.netforums.us/ have been taken down." CW-1 provided electronic copies of this information to LT Hilbolt which LT Hilbolt reviewed and verified. LT Hilbolt provided print outs of these files to SAs Lynd and Singh on 6/25/2009.

9. LT Hilbolt told Affiant that he had looked at **GhostExodus**' Craigslist post which appeared to be an ad seeking employment. This post included a summary resume with a list of security companies that **GhostExodus** had worked for. LT Hilbolt's offices conducted employment checks based on the list of Security companies and identified only one individual who had worked for all of the listed companies. Based on this, LT Hilbolt identified **GhostExodus** as **JESSE WILLIAM MCGRAW.**

Identifiers for Jesse William McGraw:

10. On 6/24/2009, SAs Allyn Lynd and Ajeet Singh conducted a search of commercial databases for **JESSE WILLIAM MCGRAW** and identified a Texas Driver's license number of 22501049, a Social Security Number of 549-93-3224, and alternate names of for **JESSE WILLIAM MCGRAW** of Howard Daniel Bertin, Howard William McGraw, Howard Rogers, and various combinations of those first middle and last names. FBI personnel retrieved a drivers license photo of **JESSE WILLIAM MCGRAW**, which

showed an address of **2801 TRINITYOAKS DR, ARLINGTON, TX, 76001.** FBI Personnel also retrieved **JESSE WILLIAM MCGRAW's** employment history and confirmed he was currently working for United Protection Services, a security firm in Dallas, Texas.

Videos of Jesse William McGraw:

11. On 6/24/2009, affiant received an email from CW-1 containing a link to a video on Youtube, a popular website where users upload homemade videos. The link http://www.youtube.com/watch?v=R_ySj_4k7RQ was to a video titled "Response to Cashis Clay's Question." Affiant reviewed the Youtube video which was posted by the user **PhantomExodizzmo**, and showed the torso and arms of an unknown male white male. The unknown male was standing behind a red, pink, grey and black speckled granite counter. In the background was a black office desk chair, short file cabinet and a green chair against a beige wall. The unknown male in the video also showed he was wearing a security guard uniform and a ballistic vest. The unknown male showed to the camera pieces of a tool kit which included: lock picking tools; a plastic card; a concealable pen video camera; a cell phone jamming device; an Acer laptop; a card reader ; two black USB thumb drives which contained "Backtrack" and "Oph Crack"(sic); and a fake FBI credential with the picture of a white male. The picture of the white male on the FBI credential appeared to match the drivers license photo of **MCGRAW**. The unknown male in the video stated the FBI credential was "good for getting into places" (sic). This video matched the description of the video of

GhostExodus showing off his "hacker gear" which CW-1 had told LT Hilbolt about. The picture shown on the fake FBI credential appeared to be of the same person as the photo of the Driver's license for **JESSE WILLIAM MCGRAW.**

12. Affiant also reviewed another video posted by the user **PhantomExodizzmo** titled "Post 4th Ops." This video showed **GhostExodus** in the process of breaking and entering into a large corporation. In it, the face of the person is clearly visible and appears to be **JESSE WILLIAM MCGRAW. MCGRAW** states the corporation does "medical stuff," **MCGRAW** shows the camera a security key card. **MCGRAW** further states he is going to compromise a computer system in the corporation with a "botnet". **MCGRAW** enters an elevator, on the elevator panel is a beige RFID security card scanner. After a few moments **MCGRAW** exits the elevator and walks down a hallway then into a stairwell. **MCGRAW** exits the stairwell stating he was now on the fifth floor. **MCGRAW** then enters an office. **MCGRAW** sits down at a desk in front of a computer LCD monitor that shows a Windows XP operating system is running on the computer connected to the monitor. On top of the monitor is a pink flamingo, a computer tower sits to the right of the monitor. On the wall in the background is a picture of what appears to be the human muscular system. **MCGRAW** is next seen accessing the Windows XP desktop of the computer. **MCGRAW** shows a USB thumbdrive which appear to the same as the USB thumbdrives in the "Response to Cashis Clay's Question video." **MCGRAW** turns the camera to the monitor which shows the Windows XP desktop. A file explorer window is open with one file in it. **MCGRAW** copies the file to the

Windows desktop then executes the file by double clicking on it. **MCGRAW** then shows the file no longer appears on the desktop. The video then switches to an IRC channel which appeared to be controlling a Bot-network. This video matches the description of CW-1 of the "infiltration video." This video shows **MCGRAW** transmitting what he describes as a malicious code to a protected computer used in the health care industry in order to cause damage to the computer in violation of 18 U. S. C. §1030. Affiant also reviewed other videos posted on Youtube by the user ETABlackOps titled "ETA member arrested" which shows **MCGRAW** in an apartment. Behind him a security guard shirt is visible and he is wearing a ballistic vest which matches the vest from the other video. **MCGRAW** states that a member of his hacking group, ETA, has been arrested, but that the cell phone for that member is still working. **MCGRAW** states that he believes that it is being used by law enforcement in an effort to gather evidence. **MCGRAW** then states that he will be sending a signal to the cell phone in an effort to destroy the evidence on it.

13. Affiant also viewed a video posted on Youtube by the user r62dl5 at the following URL http://www.youtube.com/watch?v=z3yFbcgpY9o which shows a video of **JESSE WILLIAM MCGRAW** playing the violin in the same apartment.

14. Based on the quality, field of view, mobility of the camera, and statements by **MCGRAW**, Affiant believes that all of the videos were made from the same camera, one which is either part of or attached to a laptop. **MCGRAW** also posted videos which included admonition to other hackers to assist him in conducting unauthorized computer

intrusions in support of a "massive DDOS" on 7/4/2009. Based on Affiant's knowledge, training, and experience, Affiant knows that DDOS stands for Distributed Denial of Service and is a type of computer attack in which an unauthorized individual assumes control of other computers and uses the massed ability of those computers they have unauthorized access and control over to attack targeted computers.

Residence and Vehicles:

15. On 6/24/2009. SAs Lynd and Singh spoke to the apartment manager at **2801 TRINITY OAKS DR, ARLINGTON, TX, 76001,** who confirmed that **JESSE WILLIAM MCGRAW** lives in apartment 328 based on his lease and that he and his wife had two vehicles on the lease, including a Nissan Altima. The apartment manager also provided a floor plan of apartment 328 and a verbal description of the apartment. The apartment manager also stated there was a camera over the door of apartment 328. It is Affiant's experience that computer hackers who believe that they are under surveillance or in danger of being arrested use cameras to see who is at their doors in order to destroy evidence and / or flee if law enforcement or a rival hacker come to their residence. The manager stated that apartment 328 was in the first set of apartments on the right facing Trinity Oaks Drive and across the first breezeway and up one flight of stairs on the left side of the landing.

16. Affiant drove by the apartment and was able to identify the camera above a door marked 328 one flight up from the breezeway to the building. The floor plan and verbal description provided by the manager match the apartment in the videos made by

MCGRAW. The residence is a one bedroom, one den apartment, located in the first set of apartments on the right facing Trinity Oaks Drive and across the first breezeway and up one flight of stairs on the left side of the landing and had the number 328 on a plaque on the door. There is a web camera outside the door. The building had brown brick and brown vinyl siding. While outside the apartment, SAs Lynd and Singh noted a **White Nissan Altima,** Texas License Plate DMG140. Records checks indicated that this car had Vehicle Identification Number 1N4BU31D3VC245581 and was registered to **JESSE WILLIAM MCGRAW** and his wife.

CarrellClinic:

17. On 6/24/2009, SAs Lynd and Singh travelled to the CarrellClinic, 9301 North Central Expressway, Dallas, Texas, and spoke to the building manager. While at the location, SAs Lynd and Singh recognized the guard desk in the main lobby as the desk used by **MCGRAW** in the video showing off his "hacker gear" by the counter top, a file cabinet seen behind the counter, the split level of the counter, chairs located behind the counter, and other factors. SAs Lynd and Singh also noted that the "infiltration" video made by **MCGRAW** was made at this location. SAs Lynd and Singh identified this from the hallways of the building shown in the video and the elevator shown in the video.

18. SAs Lynd and Singh also noted that the security guards at the building were from United Protective Services, the employer of **MCGRAW**. The building manager confirmed that United Protective Services provided security for the building. The building manager also told SAs Lynd and Singh that the building had recently been experiencing problems with their HVAC system. On 6/25/2009, SA Singh identified the

computer shown in the video with the pink flamingo on it inside 9301 North Central Expressway, Dallas, Texas. SA Singh was told that the computer in question was used to inprocess patients and that it was connected to all of the computers in the facility and was used in maintaining patient records, including their health records and their billing records. Property management told SA Singh that **JESSE WILLIAM MCGRAW** was assigned the nightshift from 11:00pm to 7:00am, and that he worked Tuesdays through Saturdays, with Sundays and Mondays being his off days. Further, SA Singh was told that **JESSE WILLIAM MCGRAW** did not have any authorized access to the systems on which he had placed malicious software. SA Singh was also informed that **MCGRAW** had recently provided United Protective Services with his one week notice and that his last day working for United Protective Services was 7/3/2009. Affiant recognized this date as being the day before the scheduled DDOS attack.

19. SA Singh was also told that a review of the HVAC computers had identified a malicious program on it which allowed unauthorized users to assume remote control of the system. Property management also noted that the HVAC system was continuing to experience problems, including a one hour outage of all five units controlled by the HVAC computer on 6/25/2009, which appeared to originate with the software controlling the HVAC system as none of the alarms which should have gone off did. They further noted that prior to the intrusion they have never experienced an incident where more than one or two units had problems at the same time.

Property management also told SA Singh that they had reviewed surveillance camera footage of **JESSE WILLIAM MCGRAW** arriving for work on 6/8/09, in that video, he

leaves the guard desk to go to the parking garage and returns with a blue bag and a silver aluminum attaché case which matches the one in the video where he displays his "hacker gear" and removes a laptop computer. Other staff members recalled that **JESSE WILLIAM MCGRAW** drives a small white older model **White Nissan Altima**.

20. Property management for 9301 North Central Expressway, reviewed tapes from the evening of June 25, 2009, and the morning of June 26, 2009, during the shift times for **JESSE WILLIAM MCGRAW**, and observed a light blue late model American sedan parked in the spot associated with **JESSE WILLIAM MCGRAW.** Property management sent a photo of the vehicle to Affiant. Mid morning on Friday, June 26, 2009, SA Kenneth J. Thibodeaux went to **2801 TRINITY OAKS DR, ARLINGTON, TX, 76001** and observed a 1990 light blue Oldsmobile Cutlass Ciera, bearing license MSB780, that matched the photograph provided by Property management. The tapes also show **JESSE WILLIAM MCGRAW** entering the building from the parking spot, carrying a light blue duffle back and silver attaché case. FBI personal conducted a records check of the vehicle and determined that the vehicle was registered to **JESSE WILLIAM MCGRAW**'s mother in law. The vehicle identification number was 1G3AM54N6L6369104.

Other Acts:

21. SAs Lynd and Singh also reviewed the documents provided by LT Hilbolt which CW-1 had collected. Included in these documents was what appeared to be a compromise of the City of Dallas computer system by ETA, **MCGRAW's** hacker group. Based on the naming of this system in appeared to be a computer used by Dallas Police Department's

(DPD) aviation unit. Detective Bill Cox, a DPD officer working with the FBI in a task force role, confirmed that the computer was an aviation unit computer located at or near Love Field and that it was already known by DPD to have been compromised by an unauthorized individual. Other documents indicated that **MCGRAW** had also compromised computers used by the National Aeronautic and Space Administration (NASA).

CONCLUSION

Based on the above, Affiant believes that the computers located at 9301 North Central Expressway, Dallas, Texas, are protected computers in that they are used in interstate communication and that they contain, among other things medical records. The computers located at 9301 North Central Expressway, Dallas, Texas, also control the ventilation, air conditioning, heating, etc. \

Further, that **JESSE WILLIAM MCGRAW** made unauthorized access to these computers and knowingly caused the transmission of a program, information, code, or command, that is he placed malicious software on these computers located at 9301 North Central Expressway, Dallas, Texas, and that by doing this he endangered the public health and safety. Finally, that **JESSE WILLIAM MCGRAW** plans to commit further acts of fraud relating to computers using these systems on or about 7/4/2009 all in violation of 18 U.S.C. §1030.

In light of the foregoing, Affiant believes there is probable cause to believe that violations of 18 U.S.C. §1030 have been committed by **JESSE WILLIAM MCGRAW** and that there is probable cause to believe that he plans to commit further offenses on and

before 7/4/2009.

I respectfully request that an arrest warrant be issued authorizing the arrest **JESSE WILLIAM MCGRAW** residing at 2801 TRINITY OAKS DR, APT 328 ARLINGTON, TEXAS, 76001, Texas Driver's license number 22501049, Social Security Number 549-93-3224, also known as Howard Daniel Bertin, Howard William McGraw, Howard Rogers, and various combinations of those first, middle, and last names.

Ajeet Singh, Special Agent
Federal Bureau of Investigation

SWORN TO AND SUBSCRIBED before me this 26th day of JUNE 2009.

Jeff Kaplan
United States Magistrate Judge